Computers, Materials & Continua
DOI: 10.32604/cmc.2022.025310
Article

Tech Science Press

Impact Analysis of Resilience Against Malicious Code Attacks via Emails

Chulwon Lee[1] and Kyungho Lee[2,*]

[1]Department of Information Security, Korea University, Seoul, 02841, Korea
[2]Institute of Cyber Security & Privacy, Korea University, Seoul, 02841, Korea
*Corresponding Author: Kyungho Lee. Email: kevinlee@korea.ac.kr
Received: 19 November 2021; Accepted: 09 February 2022

Abstract: The damage caused by malicious software is increasing owing to the COVID-19 pandemic, such as ransomware attacks on information technology and operational technology systems based on corporate networks and social infrastructures and spear-phishing attacks on business or research institutes. Recently, several studies have been conducted to prevent further phishing emails in the workplace because malware attacks employ emails as the primary means of penetration. However, according to the latest research, there appears to be a limitation in blocking email spoofing through advanced blocking systems such as spam email filtering solutions and advanced persistent threat systems. Therefore, experts believe that it is more critical to restore services immediately through resilience than the advanced prevention program in the event of damage caused by malicious software. In accordance with this trend, we conducted a survey among 100 employees engaging in information security regarding the effective factors for countering malware attacks through email. Furthermore, we confirmed that resilience, backup, and restoration were effective factors in responding to phishing emails. In contrast, practical exercise and attack visualization were recognized as having little effect on malware attacks. In conclusion, our study reminds business and supervisory institutions to carefully examine their regular voluntary exercises or mandatory training programs and assists private corporations and public institutions to establish counter-strategies for dealing with malware attacks.

Keywords: Cyberattack; resilience; malicious code; spear-phishing

1 Introduction

Cyberattacks are on the rise in society, owing to the COVID-19 pandemic, by 150% in the healthcare sector, 230% in the financial sector, and 350% in the phishing website [1]. According to Google reports in April 2020, there were 18 million malicious and phishing emails, and more than 240 million daily spam messages pertaining to COVID-19 [2,3]. Therefore, the damage caused by these cyberattacks has increased by 600% compared to that prior to the COVID-19 pandemic [4]. Moreover, ransomware damage from these cyberattacks occurs in all areas of society, including healthcare,

education, and finance. PCs or networks infected by malicious codes that paralyzed files in computers or network systems in organizations in the past can be easily restored by treating them. However, for-profit ransomware has recently tended to not only disable the social infrastructure and make corporate or personal data out of control for good but also expand its reach into the individual, business, and social infrastructure at large [5]. The malicious code circulates through email attachments, malicious links, and infected storage devices. In particular, the TA505 hacking group uses spear-phishing emails containing attachments with malicious code to extract information from targeted organizations or individuals [6]. According to the Symantec Internet Security Threat Report, 2019, 60% of cyber criminals used spear-phishing as the most common type of targeted attack [7]. Spear-phishing, an attempt to extort sensitive information from targeted public organizations or ask for money through ransomware, is an increasingly common type of cyberattack, the case in which hackers took down the operating technology system of the Colonial Pipeline Co. in the US and hacked confidential information from the Korea Aerospace Industries (KAI) in Korea. Therefore, detecting and blocking malicious codes in advance, which are increasingly threatening, has technical limitations. Experts are now suggesting a change in thinking that augments fast resilience from malicious code attacks rather than blocking malware attacks. Minimizing downtime and quickly restoring to the normal state are considered effective measures to respond to malware attacks through emails in the event of cyberattacks, including spear phishing attacks.

Our study contributes to finding factors influencing the effectiveness of malicious code through email in response to presentation, investigation and analysis of response modeling based on the methods of recent studies regarding malware attacks under the COVID-19 pandemic.

2 Related Works

A variety of studies have been conducted to effectively respond to malicious codes via email, such as spam prevention solution, advanced persistent threat (APT) prevention, reconsideration with information security education, counter security exercise against cyberattacks, reinforcing cyber resilience, and cyberattack visualization. Luo et al. [5] suggested a framework consisting of four stages to prevent malicious code via email. First, formulating the reaction policies and establishing a procedure to implement them. Second, reinforcing the control of banning the downloads of suspicious files through the Internet and prohibiting the reading of unidentified emails. Third, building an operating system to manage patches or updates to protect computers. Finally, improving awareness that if employees read a malicious email, it could seriously impact their customers and organizations. Alexander [8] emphasized the visualization of real-time cyberattacks to effectively respond to them as air traffic control watched the planes entering the runway in real time because it was difficult to react to invisible attacks. Lee et al. [9] developed a method to estimate the effectiveness of security event visualization to overcome the limitations of massive data analysis related to security incidents under the continuous occurrence of serious security accidents. There were several evaluation factors that include the predictability of security incidents, contents of delivery, effectiveness, immediacy, efficiency, clarity, and diversity. Furthermore, there was a difference in perspectives on the evaluation factors of visualization among managers, operators, and security consultants: managers recognized the content of delivery as the most important factor, operators consider clarity and immediacy, and security consultants recognize work efficiency. A study on the visualization of intelligence for cyber threats was in progress to collect and analyze information on cyber security threats and react to them effectively [10]. Bürkner [11] required practical exercises and simulations, such as fire drills, against cyberattacks to respond to security incidents. Resilience has been widely used in a variety of fields such as ecology, individual and organizational psychology, supply chain management, strategic

management, and safety engineering. Resilience refers to the ability to bounce back to a steady state after disruption in these fields [12–18]. Other definitions of resilience are as follows: Gallopín [19] regards system resilience as the ability to adapt to failures and security incidents, mitigate their impact, and cope with the outcomes of deformation caused by them using every available resource; Smith [20] considered cyber resilience in the context of a complicated system composed of physical, informational, cognitive, and social spheres; Kott et al. [21] considered the cyber resilience domain to consist of sensing, software, and hardware. Frenz et al. [22] proposed a plan for backup and restoration impact factors in a ransomware attack. Tab. 1 shows the key ideas of the authors.

Table 1: Comparison of related works

Category	Authors	Ideas
Malicious code email response	Luo et al. [5]	Policy and procedure, banning the downloads of suspicious files, patches, improving awareness
Effectiveness estimation	Lee et al. [9]	A method to estimate the effectiveness of response
Resilience	Gallopín [19]	System resilience
	Kott et al. [21]	Cyber resilience domain
	Bhamra et al. [12]	Idea of resilience
Visualization	Alexander [8]	Visualization of real-time cyber attacks
	Schlette et al. [10]	Visualization of intelligence for cyber threats
Exercise	Bürkner [11]	Practical exercises against cyber attacks
Backup	Frenz et al. [22]	Backup and restoration to a ransomeware attack

3 Materials and Methods

3.1 Research Model

This research model highlights the importance of resilience in responding to malicious code using email. In particular, attack visualization, practical exercise, and backup and restoration are required to improve resilience. Fig. 1 demonstrates the research model.

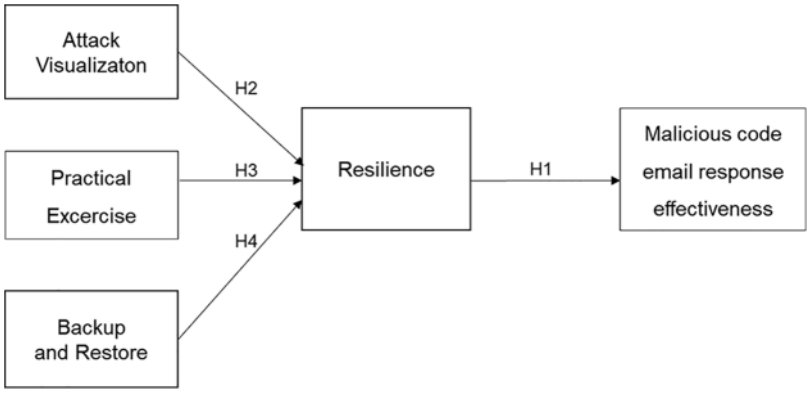

Figure 1: Research model

Effective factors for countering malicious codes include installing software such as antiviruses or blocking systems such as IPS, which has been considered important in the past, information protection education for employees, and sanctions. Other than disciplinary actions, all factors are considered effective measures that can be taken in advance before a hacking attack occurs. This proactive control is a control factor, as opposed to resilience, which weighs the recovery ability after hacking. Also, disciplinary actions can be classified as a control element to prevent recurrence after hacking incidents, unlike resilience, which aims to normalize services under hacking attacks. Three factors affecting resilience were selected because of their importance in recent studies.

The blocking of malicious code attacks through email in advance seems to have reached its limit. Therefore, rather than responding to the goal of blocking all attacks, it can be said that an approach to how quickly an attack can be returned to normal when it occurs is important. As Fig. 1 shows, the research model indicates that resilience is of paramount importance to effectively respond to malicious code attacks through email. Also, there are three factors selected on the basis of recent studies as factors significantly affecting resilience. Attack visualization points out that when a cyberattack occurs, visualizing which attack is occurring from which direction impacts resilience. Practical exercise considers that it is important for resilience in the event of an actual cyberattack to implement practical response training before a cyberattack occurs. In Backup and restore, a backup system for quick recovery in the case of failure to defend against an initial attack is considered an important factor in resilience. Tab. 2 lists detailed definitions of the terms used in the model.

Table 2: Definitions of terms

Terms	Definitions
Backup	Copying files of computer system into CD, or tapes to prepare for a system failure
Email Attack	A way of inducing users to execute a transferred hacking program through emails to invade PCs, servers, and networks
Exercise	A response test whether the employees can read and report the related emails after the emails with a hacking program are sent, and the security system can detect and block hacking programs
Malicious Code	A program to steal data or interfere with operations of PCs, servers and networks
Resilience	A recovery ability to minimize downtime of PCs, servers and networks in the event of cyberattacks
Response	Actions to block cyberattacks and restore related damages
Restore	Copying files in CD or tapes into computer systems back again in the event of malfunction
Spear-phishing	The fraudulent activity of sending emails with a hacking program to induce targeted users to click them to steal information
Visualization	The representation of positions of attackers, damaged systems, and number of attacks as an image

3.1.1 Necessity of Cyber System Resilience

The extent of damage from cyber threats is becoming large-scale and wide-ranging owing to a volatile cyber environment caused by COVID-19, as well as the improvement in internet speed and the expansion of connected devices such as IoT [2]. The Interpol Secretary General warned that cyber criminals were developing a new attack at an alarming rate using COVID-19 to exploit the fear and uncertainty caused by an unstable society and grim economic conditions [2]. There are growing concerns about the traditional approach to strengthening systems owing to the unpredictability and uncertainty caused by the swift evolution of cyber threats to systems. Thus, resilience enables systems to adapt to cyberattacks. In other words, it is important to have the ability to restore or regenerate degraded systems in the aftermath of cyberattacks [21]. Therefore, we hypothesize the following:

H1: Improving the resilience of cyber systems will have a positive effect on responding to malicious code.

3.1.2 Visualizaion of Malicious Code Email Attack

An increase in cyberattacks hampers security control by augmenting the events of security systems, such as firewalls, IPS, and antivirus software. Also, the analysis of spot cyberattacks from massive trade data is also becoming complicated owing to the increased complexity between the local system and cloud systems because of the growing use of cloud systems. Visualizing malicious code attacks is an important factor for determining them at a glance because restrictions hinder us from implementing security control practically monitoring all of them in the massive amount of log data one by one [9]. Therefore, we hypothesize the following:

H2: Visualizing malicious code attacks will have a positive effect on improving resilience.

3.1.3 Practical Excercise

Patriciu et al. [23] stated that cybersecurity exercises were very effective in protecting information. They provided practical ways to implement cyber exercises and guidelines for evaluating the indicators of the effectiveness of exercises. Kick [24] focused on having a sense of reality in scenario-based training that mixed actual events during cyber exercises. Several organizations are executing exercises for employees to respond to malicious code using email, expecting their performance. Chatchalermpun et al. [25] conducted an empirical study comparing the exercise results of phishing emails for 21,000 employees in a financial firm in Thailand. Therefore, we hypothesize the following:

H3: Practical exercises responding to malicious code using email will have a positive effect on improving resilience.

3.1.4 Backup and Restore

Frenz et al. [22] stated that the plan for backup and restoration was important for reacting to a ransomware attack. Richardson and North [26] highlighted the importance of exercise and backup in preventing ransomware attacks. Therefore, we hypothesize the following:

H4: Backup and restoration will have a positive effect on improving resilience.

3.2 Research Methods

3.2.1 Study Design and Data Collection

Structural equation modeling (SEM) was used as a multivariate method to prove the causal relationships between factors. Also, we used analysis of moment structures (AMOS) as an SEM

tool because of its convenient graphical user interface (GUI) and data compatibility with SPSS and EXCEL. Also, SEM has several advantages: controlling measurement errors, convenience of using mediating variables, and enabling statistical model evaluation [27]. Therefore, this study was conducted using SEM (see Fig. 2).

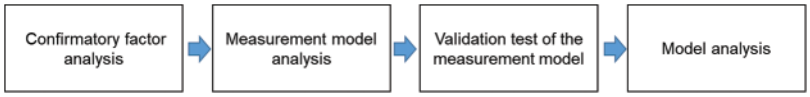

Figure 2: Process of research

Online surveys were conducted with employees of the security department in Korea using Google Forms to collect data for model verification. Among them, 100 replied to the survey, Tab. 3 shows the demographic information of the respondents.

Table 3: Demographic information of respondents

	Survey participants (N = 100)	n
Gender	Male	90
	Female	10
Age	20–29	16
	30–39	35
	40–49	44
Tenure (Years)	50 and over	5
	1–5	33
	6–10	16
	11–15	34
	16 and over	17
Position	Managerial	3
	Technical	71
	Professional staff	7
	Administrative	19
Department	Security consulting	27
	Security operation	40
	Security support	33
Task type	Security plan	18
	System operation	12
	System monitoring	28
	Security assessment	10
	Others	32
Company size	Less than 50	2
	51–200	3
	201–500	9
	501–1,000	14

(Continued)

Table 3: Continued

	Survey participants (N = 100)	n
	1,001–5,000	47
	More than 5,001	25

3.2.2 Constructs and Measurement

We used six items adopted by [9] to measure how effectively organizations could respond to malicious code attacks using emails. Six items adopted by [28] were used to measure the resilience of systems that could run properly under malicious code attacks via emails. Six items adopted by [9] were used to measure visualization of cyberattack vectors, such as its starting or destination point, and the types of attacks during malicious code attacks via emails. Six items adopted by [23,24] were used to measure the effectiveness of cyberattack response exercises against security incidents. Six items adopted by [25] were used to measure resilience to determine how effective restoration from backup data could occur during damage caused by malicious code attacks via emails (Tab. 4 lists the survey scale items).

Table 4: Survey scale items

Measurement variables	Item
Malicious code email response is adapted from [29,30]	
Response 01	The systems within the organization are sufficiently protected from malicious code.
Response 02	Malware response systems are effective.
Response 03	Most of the malware response systems have achieved their purpose.
Response 04	The malware response systems are accomplishing its most important goals.
Response 05	The malware response systems minimize damage.
Response 06	Malware is not a threat to organizations.
Resilience is adapted from [9]	
Resilience 01	Work is not interrupted even if infected with malicious code.
Resilience 02	Data infected with malware can be recovered immediately.
Resilience 03	We have enough systems and labor to recover from malware infection.
Resilience 04	We have a system that can be replaced in case of malware infection.
Resilience 05	It has independence so that it does not affect other systems even if it is infected with malicious code.
Resilience 06	Policies for restoration in case of infection with malicious code are well operated.

(Continued)

Table 4: Continued

Measurement variables	Item
Attack visualization is adapted from [9]	
Visualization 01	Visualization can predict malicious email attacks.
Visualization 02	The visualization about malicious email attack gives you an accurate understanding of the attack landscape.
Visualization 03	The visualization about malicious email attack shows us the situation intuitively.
Visualization 04	The visualization about malicious email attack increases the efficiency of work.
Visualization 05	The visualization about malicious email attack clearly shows the situation.
Visualization 06	The visualization about malicious email attack shows various information according to privileges such as administrators and operators.
Practical exercise is adapted from [23,24]	
Exercise 01	The training mail topic reflects the recent social situation well.
Exercise 01	The training mail source is similar to the actual source address.
Exercise 01	The text and images of the training mail are similar to the real mail.
Exercise 01	Training mail is related to employee work.
Exercise 01	Recovery training for malicious mail infection is well performed.
Exercise 01	Training on step-by-step actions such as reporting, and analysis is well performed.
Backup is adapted from [25]	
Backup 01	Backup and recovery plans are established in preparation for malicious code.
Backup 01	Important data on PC and server/database are well backed up.
Backup 01	Backed up data can be restored quickly.
Backup 01	Even if infected with ransomware, the backup system is backed up offline so that it is safe.
Backup 01	The backup contains the most recent point-in-time data.
Backup 01	Recovery training for backed up data is performed periodically.

4 Results

4.1 Validity and Reliability

First, we tested the unidimensionality of the measurements using confirmatory factor analysis (CFA). A valuation basis for model fit was used (see Tab. 5).

To obtain the optimal value of reliability, we deleted problematic items using the squared multiple correlation (SMC). A repeated process was used to obtain the desired result, in which the reference value was 0.4, which was less than that of SMC. Thus, we obtained the results shown in Tab. 6. The final variables were believed to satisfy reliability requirements because all constructs and measuring indicators (CMIN/DF, P, RMR, GFI, AGFI, CFI, NFI, RMESA) are fulfilled on the basis of Tab. 5.

Table 5: Reference value of Model-fit

CMIN/DF	Chi-square	GFI	AGFI	CFI	NFI	RMR	RMSEA
< 2	$P > 0.05$	≥ 0.9	≥ 0.85	≥ 0.9	≥ 0.9	≤ 0.1	≤ 0.1

CMIN: Minimum Chi-square, DF: Degree of Freedom, RMR: Root Mean-Square Residual, GFI: Goodness-of-Fit Index, AGFI: Adjusted Goodness of Fit Index, CFI: Comparative Fit Index, NFI: Normed Fit Index, RMSEA: Root Mean Square Error of Approximation.

Table 6: Results of confirmatory factor analysis (CFA)

Constructs	Numbers	CMIN	DF	P	RMR	GFI	AGFI	CFI	NFI	RMSEA
Response	6	7.710	9	.564	.029	.976	.943	1.000	.989	.000
Resilience	4	.918	2	.632	.023	.996	.978	1.000	.996	.000
Visualization	4	.932	2	.628	.020	.995	.976	1.000	.995	.000
Exercise	4	3.982	2	.137	.057	.979	.896	.983	.968	.100
Backup	4	.346	2	.841	.012	.998	.991	1.000	.999	.000

Second, our measurement model was analyzed based on the aforementioned CFA. After optimizing the adequacy of the survey questions (partly by deleting measured variables) based on the SMC values, our data yielded the following results (see Tab. 7).

Table 7: Results of the measurement model's analysis

Constructs	Measured variables	Regression weight	Standard regression weight	Standard error	CR	Measurement errors	SMC	Cronbach's alpha
Response	re2	1.000	.954	–	–	.032	.911	.970
	re3	.949	.967	.040	23.496	.025	.936	
	re4	.957	.951	.045	21.463	.031	.904	
Resilience	rs5	1.000	.830	–	–	.132	.689	.891
	rs6	1.093	.927	.095	11.469	.103	.860	
Visualization	vs3	1.000	.782	–	–	.116	.612	.851
	vs4	1.078	.809	.136	7.912	.123	.655	
	vs5	1.224	.842	.151	8.089	.143	.709	
Exercise	ex3	1.000	.957	–	–	.345	.917	.743
	ex4	.740	.623	.188	3.938	.269	.388	
Backup	bk1	1.000	.831	–	–	.130	.690	.796
	bk4	1.133	.805	.132	8.585	.182	.649	
Adequacy:	CMIN = 142.987, CMIN/DF = 1.388, P = 0.006, GFI = 0.933, AGFI = 0.889, CFI = 0.988, CFI = 0.988, RMR = 0.051, MSEA = 0.043, NFI = 0.959, IFI = 0.988							

As shown in Tab. 7, critical ratio (CR) indicates the t value, and the regression weight is significant when the value is greater than ± 1.96. Notably, all CR values are greater than 1.96. SMC indicates the ability to demonstrate the observed variables for latent variables. Therefore, SMC can tolerate variables based on a reference value of 0.4. As shown in Tab. 5, the standards for model fit are as follows: P is greater than 0.05; RMR is less than 0.05 (as well as less than 1); GFI, AGFI, CFI, NFI, and IFI are greater than 0.9; RMSEA is less than 0.08 (as well as less than 1). The results of the model analysis are acceptable because all values satisfy the reference values.

Third, a reliability analysis was performed using two tests: convergent and discriminant validity. Construct reliability was used to assess convergent validity [31], and average variance extracted (AVE) was used to assess discriminant validity [32]. Eqs. (1) and (2) was used to determine construct reliability and AVE.

$$\text{Construct Reliability} = \frac{\left(\sum \text{Standard Regression Weight}\right)^2}{\left(\sum \text{Standard Regression Weight}\right)^2 + \sum \textit{Measurement Errors}} \tag{1}$$

$$\text{AVE} = \frac{\left(\sum \text{Standard Regression Weight}^2\right)}{\left(\sum \text{Standard Regression Weight}^2\right) + \sum \textit{Measurement Errors}} \tag{2}$$

Tab. 8 presents the analysis results.

Table 8: Validation of the measurement model

Constructs	1	2	3	4	5
(1)Response	1.00				
(2)Resilience	.815	1.00			
(3)Visualization	.430	.369	1.00		
(4)Exercise	.454	.415	.260	1.00	
(5)Backup	.705	.730	.322	.363	1.00
Construct reliability	.989	.955	.929	.939	.896
AVE[a]	.969	.868	.838	.680	.811

[a] Average variance extracted

The results showed that convergent validity was demonstrated with construct reliability values (0.896 to 0.989 for all constructs greater than 0.7). Moreover, discriminant validity is demonstrated because the AVEs (0.680 to 0.969) of all variables are greater than the largest correlation coefficient (resilience: 0.815) of the square root (0.664) [32].

4.2 Result of Analysis

Malware attacks via emails have grown in number in the following ways: ransomware cyberattacks on organizations and social infrastructures, and information capture through spear-phishing attacks. According to several experts, resilience has emerged owing to the limitations of advanced prevention systems in the face of a variety of efforts to tackle the damages caused by malicious email attacks. Thus, we established a new model to demonstrate the relationship among three factors: attack visualization, practical exercise, and backup and restore, which affected resilience against malware attacks via email. As Tab. 9 shows, the estimates from SEM were within tolerable levels for the proposed model, such that CMIN = 38.565, CMIN/DF = 0.838, P = 0.774, GFI = 0.939, AGFI = 0.897, CFI = 1.000,

RMR = 0.065, RMSEA = 0.000, NFI = 0.961, and IFI = 1.008. Therefore, the model fit was appropriate for comparison with reference values (CMIN/DF < 2, P > 0.05, GFI ≥ 0.9, AGFI ≥ 0.85, CFI ≥ 0.9, NFI ≥ 0.9, RMR ≤ 0.1, and RMSEA ≤ 0.1).

Table 9: Results of the model

Path (Hypothesis)	Estimate	CR[a]	P[b]
Resilience -> Response (H1)	.880	9.849	***
Attack Visualization -> Resilience (H2)	.152	1.691	.091
Practical Exercise -> Resilience (H3)	.105	.898	.369
Backup and Restore -> Resilience (H4)	.774	6.102	***
Model Fit[c]	CMIN = 142.987, CMIN/DF = 1.388, P = 0.006, GFI = 0.933, AGFI = 0.889, CFI = 0.988, RMR = 0.051, RMSEA = 0.043, NFI = 0.959, IFI = 0.988		

[a]CR >± 1.96, [b]p < 0.05, [c]Model fit reference value: CMIN/DF (< 2), p (> 0.05), GFI (≥ 0.9), AGFI (≥ 0.85), CFI (≥ 0.9), NFI (≥ 0.9), RMR (≤ 0.1), RMSEA (≤ 0.1).

The test results of the proposed hypotheses H1 and H4 were supported within the 95% confidence interval with P < 0.05, and C.R. >± 1.96. Thus, backup and restoration has a positive effect on improving resilience, which positively affects responses against malicious code attacks via emails. However, the proposed hypotheses H2 and H3 are not supported, with P > 0.05 and C.R. <± 1.96. Thus, attack visualizaton and practical exercise did not influence resilience (see Fig. 3).

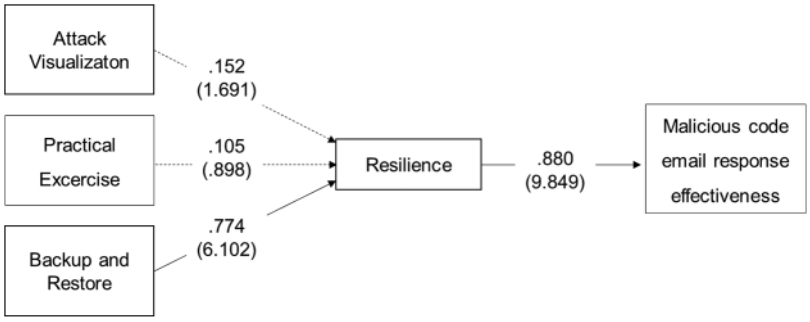

Figure 3: Results of the model, All path coefficients are standardized estimates corresponding to P < 0.05, and CR >± 1.96. Note that the CR values are within parentheses. Grayed-out arrows indicate that the hypotheses are not supported

5 Discussion

Our study investigated the effectiveness of resilience, attack visualization, practical exercise, and backup and restoration, which recently became important in response to malicious code emails. Because only the necessity of each factor was mentioned in the previous study, we newly investigated how each factor interacted with the effectiveness of the response against malicious codes through resilience. To this end, we used a confirmatory research method using SEM. The results showed that resilience, backup and restoration were effective in responding to malicious code email; however, attack

visualization and practical exercise had no meaningful effect. Attack visualization did not have a considerable effect because the attack visualization solutions currently used by companies did not show the attack situation properly. In other words, the current technology for attack visualization did not provide a function that was beneficial to security practitioners. Moreover, in the case of practical exercise, employees became insensitive to training due to frequent exercise. Therefore, our study showed that attack visualization technology required to be improved effectively to assist security practitioners in responding, and the email response exercise required to be completely reformed.

5.1 Research Contributions

As malicious code email attacks have become more intelligent and expanding, experts continue to argue that resilience is required in addition to the existing defense system, which is verified by our research. Meanwhile, companies in Korea are also conducting regular email mock training to block malicious code emails, and various policies are in place, such as mandatory submission of response training results to supervisory authorities once a year; however, the current method required to be changed. Furthermore, our study show that resilience is important for effectively responding to malicious code emails, which requires backup. Therefore, it is meaningful to provide a rationale for companies to build a more robust backup system. In addition, it is necessary to review policies for offline backup and real-time backup in preparation for ransomware.

5.2 Limitations and Future Research

This study had several limitations. First, it was based on a subjective evaluation of employees performing information protection work in Korea. Therefore, different countries might have different results depending on the region.

Second, because this study was modeled mainly based on resilience, which had been frequently mentioned recently in the field of information protection, all factors that were effective in responding to malicious code might not have been reviewed.

Third, the effects of attack visualization and practical exercise were found to be insignificant in this study. Therefore, the subject of future research might be regarding the factors that increased the effectiveness of attack visualization and practical exercise.

Malicious code and distributors have become increasingly intelligent, and they rapidly take advantage of recent social phenomena. Therefore, when a new technology appears or a change in the social environment appears in the future, the method of dealing with malicious code might change; thus, new studies reflecting such trends must be continued in the future.

6 Conclusions

Owing to the impact of COVID-19, non-face-to-face activities have increased, due to which malicious code attacks such as ransomware and spear-phishing have grown in number, along with advancements in their technology. Various technical control devices such as the existing spam mail blocking solution, APT blocking system, and email isolation solution are being installed and running to block malicious code email. However, we are facing a situation that makes it incapable to completely block the emails using these technical control measures, and experts are calling for a paradigm change regarding resilience. Therefore, we developed a malware response model that fits this new paradigm, collected data from 100 information protection experts in Korea using a Google survey, and tested our model through SEM to ensure that resilience and backup were effective in responding to malicious

code emails. Therefore, it is expected that our research will be of remarkable interest for establishing a strategy to deal with malicious code attacks.

Acknowledgement: The authors would like to thank Editage (https://www.editage.co.kr) for their English language editing.

Funding Statement: This study was supported by a grant from the Korean Health Technology RD Project, Ministry of Health and Welfare, Republic of Korea (HI19C0866).

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding this study.

References

[1] H. E. K. Alsabti, "Cyberspace: What now, what next?" in *Global Cybersecurity Forum. 2nd Int. Forum, GCF 2021, Proc.: Opening Remarks*, Riyadh, Saudi Arabia, NCA, 2021. [Online]. Available: https://www.youtube.com/watch?v=WhUNP7omPHQ&t=940s.

[2] K. B. Alexander and J. N. Jaffer, "COVID-19 and the cyber challenge," *Cyber Defense Review*, vol. 6, no. 2, pp. 17–28, 2021.

[3] S. Musil, in *Google Blocking 18m Malicious Coronavirus Emails Everyday*, San Francisco, CA, USA: CNET, 2020. [Online]. Available: https://www.cnet.com/tech/services-and-software/google-seeing-18m-malicious-coronavirus-emails-each-day/.

[4] R. Sobers, in *81 Ransomware Statistics, Data, Trends and Facts for 2021*, New York City, USA: VARONIS, 2021. [Online]. Available: https://www.varonis.com/blog/ransomware-statistics-2021.

[5] X. Luo and Q. Liao, "Awareness education as the key to ransomware prevention," *Information Systems Security*, vol. 16, no. 4, pp. 195–202, 2007.

[6] Y. Jeong, M. Lee, K. Kim, J. Kim, M. Park *et al., Cyber Threat Intelligence Report*. Seoul, Korea: Korea Financial Secuirity Institute, 2021. [Online]. Available: https://www.fsec.or.kr/common/proc/fsec/bbs/163/fileDownLoad/2298.do.

[7] B. O'Gorman, C. Wueest, D. O'Brien, G. Cleary, H. Lau *et al., Internet Security Threat Report*. Mountain View, CA, USA: Symantec, 2019. [Online]. Available: https://docs.broadcom.com/doc/istr-24-2019-en.

[8] K. Alexander, "Cyberspace: What now, what next?," in *Global Cybersecurity Forum. 2nd Int. Forum, GCF 2021, Proc.: Cyber Industry Review*, Riyadh, Saudi Arabia: NCA, 2021. [Online]. Available: https://www.youtube.com/watch?v=WhUNP7omPHQ&t=940s.

[9] M. Lee and K. Lee, "Decision model of the effectiveness for advanced that security visualization," *Journal of the Korea Institute of Information Security & Cryptology*, vol. 27, no. 1, pp. 147–162, 2017.

[10] D. Schlette, F. Böhm, M. Caselli and G. Pernul, "Measuring and visualizing cyber threat intelligence quality," *International Journal of Information Security*, vol. 20, no. 1, pp. 21–38, 2021.

[11] H. Bürkner, "Cyberspace: What now, what next?" in *Global Cybersecurity Forum. 2nd Int. Forum, GCF 2021, Proc.: Unlocking the Challenges and Opportunities of Cyberspace*, Riyadh, Saudi Arabia: NCA, 2021. [Online]. Available: https://www.youtube.com/watch?v=WhUNP7omPHQ&t=940s.

[12] R. Bhamra, S. Dani and K. Burnard, "Resilience: The concept, a literature review and future directions," *International Journal of Production Research*, vol. 49, no. 18, pp. 5375–5393, 2011.

[13] B. Walker, S. Carpenter, J. Anderies, N. Abel, G. Cumming *et al.,* "Resilience management in social ecological systems: A working hypothesis for a participatory approach," *Conservation Ecology*, vol. 6, no. 1, 2002. https://www.researchgate.net/publication/312974957_Resilience_management_in_social-ecological_systems_a_working_hypothesis_for_a_participatory_approach.

[14] C. K. Barnett and M. G. Pratt, "From threat-rigidity to flexibility-toward a learning model of autogenic crisis in organizations," *Journal of Organizational Change Management*, vol. 13, no. 1, pp. 74–88, 2000.

[15] E. H. Powley, "Reclaiming resilience and safety: Resilience activation in the critical period of crisis," *Human Relations*, vol. 62, no. 9, pp. 1289–1326, 2009.
[16] M. Christopher and H. Peck, "Building the resilient supply chain," *International Journal of Logistics Management*, vol. 15, no. 2, pp. 1–13, 2004.
[17] G. Hamel and L. Valikangas, "The quest for resilience," *Harvard Business Review*, vol. 81, no. 9, pp. 52–63, 2003.
[18] E. Hollnagel, D. D. Woods and N. Leveson, "Defining resilience," in *Resilience Engineering: Concepts and Precepts*, Boca Raton, FL, USA: CRC Press, pp. 31–40, 2006.
[19] G. C. Gallopín, "Linkages between vulnerability, resilience, and adaptive capacity," *Global Environmental Change*, vol. 16, no. 3, pp. 293–303, 2006.
[20] E. A. Smith, "Shaping behavior: operations in the cognitive domain," in *Effects Based Operations: Applying Network Centric Warfare in Peace, Crisis, and War*, Arlington, VA, USA: DOD-CCR Press, pp. 157–191, 2003.
[21] A. Kott and I. Linkov, "Fundamental concepts of cyber resilience: introduction and overview," in *Cyber Resilience of Systems and Networks*, Cham, ZG, Switzerland: Springer International Publishing, pp. 1–25, 2019.
[22] C. M. Frenz and C. Diaz, "Backup," in *Anti-ransomware Guide*, Wakefield, MA, USA, pp. 9–10, 2017. [Online]. Available: https://owasp.org/www-pdf-archive/Anti-RansomwareGuidev1-7.pdf.
[23] V. V. Patriciu and A. C. Furtuna, "Guide for designing cyber security exercises," in *E-Activities and Information Security and Privacy, 8th Int. Conf., World Scientific and Engineering Academy and Society (WSEAS)*, Wisconsin, USA, pp. 172–177, 2009.
[24] J. Kick, "Exercise Outcomes," in *Cyber Exercise Playbook*, Bedford, MA, USA: MITRE CORP, pp. 5–7, 2014. [Online]. Available: https://apps.dtic.mil/sti/citations/ADA624910.
[25] S. Chatchalermpun, P. Wuttidittachotti and T. Daengsi, "Cybersecurity drill test using phishing attack: a pilot study of a large financial services firm in Thailand," in *Computer Applications & Industrial Electronics (ISCAIE), IEEE 10th Symp.*, Piscataway, NJ, USA: IEEE, pp. 283–286, 2020.
[26] R. Richardson and M. M. North, "Ransomware: Evolution, mitigation and prevention," *International Management Review*, vol. 13, no. 1, pp. 10–21, 2017.
[27] H. Kang and J. Ahn, "Model setting and interpretation of results in research using structural equation modeling: A checklist with guiding questions for reporting," *Asian Nursing Research*, vol. 15, no. 3, pp. 157–162, 2021.
[28] J. Choi, W. Kim and J. Lim, "A study on maturity model for the assessment of cyber resilience level in the defence information system," *Journal of the Korea Institute of Information Security & Cryptology*, vol. 29, no. 5, pp. 1153–1165, 2019.
[29] C. Lee and K. Lee, "Factors affecting corporate security policy effectiveness in telecommuting," *Security and Communication Networks*, vol. 2021, 2021.
[30] J. S. Hsu, S. P. Shih, Y. W. Hung and P. B. Lowry, "The role of extra role behaviors and social controls in information security policy effectiveness," *Information Systems Research*, vol. 26, no. 2, pp. 282–300, 2015.
[31] J. F. Hair, R. E. Anderson, R. L. Tatham and W. C. Black, "Confirmatory factor analysis," in *Multivariate Data Analysis: A Global Perspective*, 7th ed., vol. 5. Hoboken, NJ, USA: Prentice Hall, pp. 661–699, 2009.
[32] C. Fornell and D. F. Larcker, "Evaluating structural equation models with unobservable variables and measurement error," *Journal of Marketing Research*, vol. 18, no. 1, pp. 39–50, 1981.